vicarius

vRx vRadar

Network Scan

The network scan identifies open ports, active services, and operating systems across live hosts, mapping the network-facing characteristics of each device, the foundation for deeper vulnerability and compliance assessments.

How it works

1. **TCP & UDP port scan** - Checks each host for open ports using SYN scans (TCP) and probe-based discovery (UDP).
2. **Service identification** - Banner grabbing and protocol negotiation to identify software and version.
3. **OS fingerprinting** - TCP/IP stack analysis via integrated Nmap (-O) and Xprobe2 for OS and kernel version.
4. **Network enumeration** - Queries DNS, RPC, SNMP, and shared filesystems for additional context.
5. **Scan policy tuning** - Fully tunable timing, port range, depth, and aggressiveness.

What you get

- **Open Ports: Full TCP/UDP port list per host**
- **Services: Application and version per port**
- **OS Details: Operating system and kernel version**
- **Network Metadata: DNS, shares, SNMP info**
- **Attack Surface Map: Input for vulnerability scans**

Why it's important

- **Reveals all externally reachable entry points**
- **Detects rogue or unauthorized services on the network**
- **Validates segmentation and firewall enforcement**

Comparison to Competitors

Feature	vRadar	Nessus / Tenable	Qualys	Rapid7	OpenVAS
Port Scan Depth	**Full TCP/UDP range**	Fixed templates	Preset cloud range	Fast, less deep	Configurable, slow
Service ID	**Deep banner analysis**	Common svc focus	Limited, cloud sync	Basic port mapping	Plugin-dependent
OS Fingerprinting	**Dual-engine (Nmap + Xprobe2)**	Single proprietary	Internal logic only	Simplified detect	Outdated fingerprints
Network Enum	**DNS, RPC, SNMP, shares**	Common data only	Agent-reported only	Basic data only	Plugin-dependent
Scan Policy Ctrl	**Full tuning options**	Fixed templates	Centralized only	Automated presets	Manual, complex